

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): NISHIZAWA, et al

Serial No.:

Filed: August 30, 2001

Title: DATABASE ACCESS METHOD SYSTEM CAPABLE OF  
CONCEALING THE CONTENTS OF QUERY

Group:



LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of  
Patents and Trademarks  
Washington, D.C. 20231

August 30, 2001

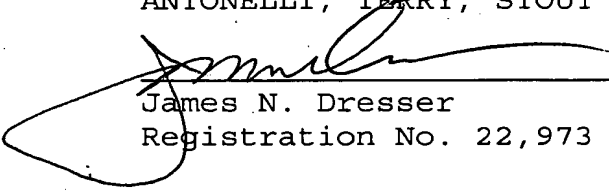
Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2001-017827 filed January 26, 2001.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

  
James N. Dresser  
Registration No. 22,973

JND/nac  
Attachment  
(703) 312-6600

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

JC997 U.S. PTO  
09/941850



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application:

2001年 1月26日

出 願 番 号  
Application Number:

特願2001-017827

出 願 人  
Applicant(s):

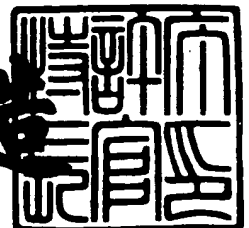
株式会社日立製作所

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 6月11日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 H00013031A

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/30

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

【氏名】 西澤 格

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

【氏名】 牛嶋 一智

【発明者】

【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目 2 8 0 番地 株式会社日立製作所中央研究所内

【氏名】 新谷 隆彦

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社 日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【電話番号】 03-3212-1111

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1  
【物件名】 要約書 1  
【ブルーフの要否】 要

## 【書類名】明細書

【発明の名称】問合せ内容を隠蔽するデータベースアクセス方法およびシステム

## 【特許請求の範囲】

## 【請求項 1】

ユーザからの処理要求を受け付ける少なくとも 1 個のクライアント計算機システム（以下、クライアント）と、それぞれにデータベースを備え上記クライアントからのアクセス要求に従って上記データベースを検索する少なくとも 1 個のサーバ計算機システム（以下、サーバ）と、各クライアントを所望のサーバに接続するネットワークと、クライアントと前記ネットワークの間に接続され、クライアントからの処理要求をサーバに転送しデータを収集する機能を有する少なくとも 1 個のデータ中継機構とを備え、上記データ中継機構は、前記クライアントからの要求を解析する問合せ解析部と、解析した問合せを暗号化する暗号化問合せ生成部と、前記サーバ上の前記データベースのデータを暗号化する暗号化プログラム作成部と、上記暗号化問合せおよび上記暗号化プログラムを適切なサーバに発行するための問合せおよび暗号化プログラム発行部と、サーバより取得した結果の統合処理を行う結果統合部とを含むことを特徴とするデータ中継機構。

## 【請求項 2】

請求項 1 に記載のデータ中継機構であって、上記データ中継機構は、前記クライアントからの要求を解析する問合せ解析部と、解析した問合せを他の問合せと結合した結合問合せ、もしくは解析した問合せを協調するデータ中継機構に分配するための分配問合せに変換する問合せ変換部とを含むことを特徴とするデータ中継機構。

## 【請求項 3】

請求項 1 に記載のデータ中継機構であって、上記データ中継機構は、前記クライアントからの要求を解析する問合せ解析部と、サーバのデータベースが保持するデータの一部を保持するキャッシュデータベースと、前記問合せが前記キャッシュデータベース内のデータを用いて処理可能な場合に、上記問合せを実行する問合せ実行部とを含むことを特徴とするデータ中継機構。

## 【請求項 4】

データベースを備え、クライアント計算機からのアクセス要求に従って上記データベースを検索するサーバ計算機システム（以下、サーバ）であって、上記サーバは、データを保持するデータベースと、上記データベースを管理し問合せを受け付けるデータ管理・検索部と、データベース内のデータにアクセスするデータアクセス部とを含み、前記データ管理・検索部は、受け付けた問合せが暗号化されている場合に、問合せ発行元の計算機もしくは暗号化プログラムサーバから暗号化プログラムを受け取り、前記データアクセス部は、前記データベースに保持するデータを前記暗号化プログラムで暗号化を施しながら読み出し、上記データベースを検索する機能を有することを特徴とするサーバ計算機システム。

【請求項5】

データを保持するデータベースを管理し、問合せを受け付けるデータ管理・検索部と、データベース内のデータにアクセスするデータアクセス部とを有するデータベースシステムであって、暗号化された問合せと、暗号化プログラムが与えられた場合に、データ管理・検索部でデータを検索する処理において、データアクセス部で、データを格納するデータベースのデータを読み出す際に暗号化プログラムを適用して問合せの照合を行うことを特徴とするデータ管理・検索システム。

【請求項6】

ユーザからの問合せを受け付け、上記問合せに対するデータの検索結果を返す情報提供サービス方法において、ユーザの問合せに含まれる機密条件を解読しないことを保証する情報提供サービス方法。

【請求項7】

クライアント計算機システム（以下、クライアント）からの問合せを受け付け、適切な情報提供サービスが稼動するサーバ計算機システム（以下、サーバ）に問合せを転送する、問合せ仲介サービス方法において、ユーザの問合せに含まれる機密条件を解読しないことを保証する情報提供サービスが稼動する前記サーバにのみ問合せを転送することを特徴とする問合せ仲介サービス方法。

【請求項8】

クライアント計算機システム（以下、クライアント）からの問合せを受け付け

、適切な情報提供サービスが稼動するサーバ計算機システム（以下、サーバ）に問合せを転送する、問合せ仲介サービスにおいて、複数の前記情報提供サービスの課金情報を収集して対価をまとめて支払い、その後前記クライアントの前記問合せ毎の課金情報を生成して、各クライアントから対価を得ることを特徴とする課金方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ユーザもしくはアプリケーションから投入される問合せの内容を隠蔽するデータ中継機構、サーバ計算機システム、データベースシステムおよびその方法に関する。

【0002】

【従来の技術】

インターネットをはじめとするネットワーク技術の進歩と普及により、多数の計算機がネットワークに接続されるようになっている。これに伴い、さまざまな情報をネットワーク経由で提供する情報提供サービスが広く利用されつつある。例えば、特許情報検索サービスや遺伝子配列情報検索サービスがその好例である。

【0003】

これらの情報提供サービスを利用するユーザは、さまざまな計算機からネットワーク経由で情報提供サービスが稼動する計算機に対してアクセスを行う。以下では前記ユーザが利用する計算機をクライアント計算機、前記情報提供サービスが稼動する計算機をサーバ計算機と呼ぶこととする。現状ではクライアント計算機としては、ワークステーション、パーソナルコンピュータ、小型の携帯端末、そして携帯電話が、サーバ計算機としては、メインフレームやUNIXサーバ、PCサーバが利用されることが多い。

【0004】

また、前記情報提供サービスへのアクセスに際して、ユーザはクライアント計算機上で専用のソフトウェアやWEBブラウザを利用し、情報提供サービスが稼

動するサーバ計算機上でのデータの管理および検索はデータベース管理システム（以下、DBMS）を用いて行われるのが普通である。

【0005】

前記情報提供サービスへのアクセスにおいて、例えば遺伝子配列情報や特許情報を検索する場合に、「誰が」「どのような条件」で情報にアクセスしたかを隠蔽したいというように、ユーザがアクセスの匿名性、検索内容の秘密性を保持したい場合がある。これは、遺伝子配列検索や特許キーワード検索等、問合せに指定される条件自体が機密の対象であり、これらの機密を隠蔽したまま検索を行うことが重要となる場合があるためである。

【0006】

従来のセキュリティ技術では、（１）ネットワーク上での盗聴に対する情報の保護、（２）アクセスを行うユーザのサーバ側での認証などが実現されている。また、それらの実現方法としては、通信を行うクライアント計算機とサーバ計算機間で例えばSSL（Secure Socket Layer）などの暗号化プロトコルを用いる方法や、図2に示すような方法がある。すなわち図2においては、クライアント計算機201で問合せを暗号化し、暗号化した問合せ202をネットワーク203経由で前記情報提供サービスが稼動するサーバ計算機205に転送し、上記サーバ計算機ではネットワークインタフェース部206経由で、前記暗号化問合せを問合せ復号部210に送り、上記問合せ復号部で前記暗号化問合せを復号してDBMS208でデータベース211に対して検索を行う。そして検索の結果207を前記ネットワークインタフェース、および前記ネットワーク経由でクライアント計算機に転送する。

【0007】

しかし、上述の方法ではネットワーク上で暗号化されている問合せも、サーバ内では復号されてから検索処理が行われるため、ユーザの検索内容はサーバ計算機に対しては隠蔽されない。そのため、機密を含む検索内容が悪意を持つサーバ側の管理者に漏洩する危険があり、問合せに指定される条件自体が機密対象である場合に、これらの機密を隠蔽したまま検索を行うことは困難であった。

【0008】



すなわち、図3に示すネットワーク経由の問合せ処理において、サーバが信用でき、かつ検索内容を知られても構わず（ステップ302でYesが選択された場合）、信用できる通信路が存在しない場合（ステップ303でNoが選択された場合）には、クライアントで問合せを暗号化し、サーバで上記問合せを復号して検索（ステップ306）することで対応でき、サーバが信用でき、かつ検索内容を知られても構わず、さらに信用できる通信路が存在する場合（ステップ303でYesが選択された場合）には、問合せの暗号化自体を行う必要がないので問題は生じない。しかしながら、前記のサーバに対して問合せの内容を隠蔽したい場合は、図3のステップ305に相当する場合であり、従来の方法では対応が困難であった。

## 【0009】

特開平11-259512「データ検索システム」（文献1）では、ユーザから入力された問合せの条件に対し、（1）登録した機密項目に関する条件を削除、（2）条件値の包含関係（概念階層）を利用して条件値を変換、そして（3）代行サーバ利用により、検索サーバでのトレースによるユーザの検索内容、所在の機密を保護するシステムを提供している。本従来例によれば、ユーザの情報の一部はサーバに対して隠蔽が可能となるが、検索条件がサーバに取得されるという問題と、名前や遺伝子配列など、条件値の包含関係の拡大が困難な場合が多く、適用対象が限定されるという問題があった。

## 【0010】

特開昭64-14665「住民基本台帳ファイル方式」（文献2）では、住民基本台帳データの入力時に、住民基本台帳データを暗号化し、上記暗号化データを格納することにより、悪意を持つ者が住民台帳ファイルをアクセスし、個人情報取得するのを防止する。本従来例では、暗号化されたデータに対してユーザの問合せのマッチングを行う際に格納データの復号処理を行うため、ユーザの問合せはサーバ側では隠蔽されず、サーバ側の管理者に悪意がある場合にはその問合せ内容を知られてしまう。

## 【0011】

特開平11-272681「個人情報の記録方法およびその記録媒体」（文献

3)においては、「前記文献2の方法では、データ復号化に伴う処理効率低下、および暗号化の方法によっては大小関係が保持できないことにより、検索不可の条件が生ずる等の問題がある」との指摘がなされている。そのため、文献3の発明では(1)個人情報を、基本データ項目を格納する基本情報ファイルと、それ以外を格納する属性情報ファイル群に分割し、(2)個人情報を特定する個人コードで上記のファイル間の関連付けを行い、(3)必要に応じて、関連付けを行う個人コードを暗号化することにより、データ全体を暗号化する必要があるようにして前記問題を回避する提案がなされている。しかしながら、本従来例でも文献2の技術と同様に、検索時にユーザが投入する条件は暗号化されないため、サーバ側で上記条件が漏洩する危険を伴う。

## 【0012】

米国特許5963642 “Method and apparatus for secure storage of data” (文献4)では、データベースに格納するデータ自体をビットマップ化し、ユーザの問合せは同様のビットマップに変換して検索することにより、上記問合せを復号することなく検索を行うことができる。しかしながら、本従来例ではサーバのデータを予め全てビットマップにエンコードしておく必要があり、既存のデータベースに対して本方式を適用するのは困難である。

## 【0013】

## 【発明が解決しようとする課題】

従来技術においては、ユーザがクライアント計算機からネットワークを介してサーバ計算機上で稼動する情報提供サービスを利用する場合に、クライアント計算機側で入力する機密を含む条件を隠蔽したまま、サーバ計算機上のシステムで検索を行うことは困難であった。

## 【0014】

本発明の第1の目的は、ユーザが保護したい条件を隠蔽したまま情報提供サービスを利用する方法およびシステムを提供することである。また本発明の第2の目的は、条件を隠蔽したまま情報を提供するサービスと上記サービスを実現するためのプロトコルを提供することである。さらに、本発明の第3の目的は、前記ユーザが保護したい条件を隠蔽したまま情報提供サービスを利用する方法および

システムの性能を向上させる機構を提供することである。

【 0 0 1 5 】

【課題を解決するための手段】

本発明では、前記第 1 および第 2 の目的を達成するため、(1) ユーザがクライアント計算機に対して投入した問合せを変換し、上記問合せとサーバ計算機で実行される問合せの対応関係を変化させることによって問合せの内容、および問合せ発行位置を隠蔽し、(2) 問合せの暗号化対象項目を暗号化した暗号化問合せを作成し、サーバ計算機では上記暗号化問合せを復号せずに、検索対象のデータを問合せと同様に暗号化しながら検索を行うことにより、サーバ計算機側でユーザの投入した問合せが含む機密情報を隠蔽することを可能とした。

【 0 0 1 6 】

また、本発明では前記第 3 の目的を達成するため、(1) サーバ計算機に転送する暗号化プログラムを問合せにさきがけて予め転送し、暗号化済みのデータを生成する、もしくは(2) データ中継機構内に、問合せ結果をキャッシングする機構を準備し、問合せ処理で利用するという機構を備える。

【 0 0 1 7 】

【発明の実施の形態】

本発明の情報提供サービスを実施するシステムの好適な構成は、データ検索ユーザからの処理要求を受け付ける少なくとも 1 個のクライアント計算機システム(以下、クライアント)と、それぞれにデータベースを備え上記クライアントからのアクセス要求に従って上記データベースを検索する少なくとも 1 個のサーバ計算機システム(以下、サーバ)と、各クライアントを所望のサーバに接続するネットワークと、クライアントと前記ネットワークの間に接続され、クライアントからの処理要求をサーバに転送しデータを収集する機能を有する少なくとも 1 個のデータ中継機構とを備える。そして上記データ中継機構は、前記クライアントからの要求を解析する問合せ解析部と、解析した問合せを暗号化する暗号化問合せ生成部と、前記サーバ上の前記データベースのデータを暗号化する暗号化プログラム作成部と、上記暗号化問合せおよび上記暗号化プログラムを適切なサーバに発行するための問合せおよび暗号化プログラム発行部と、サーバより取得し

た結果の統合処理を行う結果統合部とを含む。

【0018】

また、上記構成のデータ中継機構は、前記クライアントからの要求を解析する問合せ解析部と、解析した問合せを他の問合せと結合した結合問合せ、もしくは解析した問合せを協調するデータ中継機構に分配するための分配問合せに変換する問合せ変換部とを含むことがある。

【0019】

また、上記データ中継機は、前記クライアントからの要求を解析する問合せ解析部と、サーバのデータベースが保持するデータの一部を保持するキャッシュデータベースと、前記問合せが前記キャッシュデータベース内のデータを用いて処理可能な場合に、上記問合せを実行する問合せ実行部とを含むことがある。

【0020】

また、本発明を実施するサーバ計算機システムは、データを保持するデータベースと、上記データベースを管理し、問合せを受け付けるデータ管理・検索部と、データベース内のデータにアクセスするデータアクセス部とを含み、前記データ管理・検索部は、受け付けた問合せが暗号化されている場合に、問合せ発行元の計算機もしくは暗号化プログラムサーバから暗号化プログラムを受け取り、前記データアクセス部は、前記データベースに保持するデータを前記暗号化プログラムで暗号化を施しながら読み出す機能を有し、クライアント計算機からのアクセス要求に従ってデータベースを検索する。

【0021】

また、本発明のデータ管理・検索システムは、上記データを保持するデータベースを管理し、問合せを受け付けるデータ管理・検索部と、データベース内のデータにアクセスするデータアクセス部とを有するデータベースシステムであって、暗号化された問合せと、暗号化プログラムが与えられた場合に、データ管理・検索部でデータを検索する処理において、データアクセス部で、データを格納するデータベースのデータを読み出す際に暗号化プログラムを適用して問合せの照合を行う。

【0022】

本発明の好適な実施形態を図1に示す。図1ではクライアント計算機1（101）およびクライアント計算機2（102）がネットワーク127を介してデータ中継機構105に接続されている。上記ネットワーク127は、イーサネット、光ファイバ、FDDIで接続されるローカルエリアネットワーク（LAN）、もしくはLANよりも低速なインターネットを含んだワイドエリアネットワーク（WAN）でも差し支えない。

## 【0023】

通常、ユーザはクライアント計算機上で稼動する専用プログラムもしくはブラウザを利用してシステムに対して問合せを発行し、上記問合せに対する結果を取得するため、以降の説明では問合せの発行元、最終結果の取得先をクライアント計算機と考えることとする。クライアント計算機は、（株）日立製作所のHitachi FLORAなどのパーソナルコンピュータ、（株）日立製作所のHitachi 3500ワークステーションなどの任意のコンピュータシステム、（株）日立製作所のPersonaなどの携帯端末、もしくは問合せインタフェースを持つ携帯電話でも差し支えない。

## 【0024】

また、クライアントが接続されるデータ中継機構105、114および情報提供システムが稼動するサーバ計算機119は、（株）日立製作所のHitachi 3500ワークステーションなどの任意のコンピュータシステムでよい。さらに、サーバ計算機上で稼動する前記情報提供システムがデータ管理、および検索に利用するデータ管理・検索部124は、（株）日立製作所のHiRDB、オラクル（Oracle）社のOracle 8、IBM社DB2などの汎用DBMS製品で差し支えない。

## 【0025】

データ中継機構間を結ぶネットワーク113、およびデータ中継機構とサーバ計算機を結ぶネットワーク117は、イーサネット、光ファイバ、FDDIで接続されるローカルエリアネットワーク（LAN）、もしくはLANよりも低速なインターネットを含んだワイドエリアネットワーク（WAN）でも差し支えなく、ネットワーク114、117、および127は異なるネットワークであっても

、同一のネットワークであってもよい。

【 0 0 2 6 】

本実施例ではデータ中継機構には2つのクライアント計算機が接続されているが、クライアント計算機の数はい任意で構わない。さらに、本実施例ではクライアント計算機が小型の携帯端末や携帯電話等、記憶装置容量、計算能力、バッテリー能力の制限から余分な処理機構を搭載できない場合を考慮してデータ中継機構を用いているが、前記制限がない場合にはクライアント計算機に以下で説明するデータ中継機構中の処理の一部または全部を備えても差し支えない。

【 0 0 2 7 】

受け付けられた問合せ103は問合せ解析部106によって解析され、データ中継機構のキャッシュデータベース128中のデータを用いて処理が可能か否かが判定される。上記解析および判定の方法は、特願平11-285164（文献5）に開示された部分レプリカの利用方法を適用すればよい。前記キャッシュデータベースが存在しない場合、もしくは前記キャッシュデータベース中のデータが利用できないと判定された場合には、前記問合せは問合せ変換部107に送られる。

【 0 0 2 8 】

問合せ変換部107での処理を図6のフローチャートを用いて説明する。問合せ変換部では問合せを受け付けた（ステップ602）後、問合せ連結を行うか否かを判定する（ステップ603）。問合せ連結とは、複数の問合せを連結する処理で、同一クライアント計算機から発行された問合せのみならず、異なるクライアント計算機から発行された問合せもその対象となる。問合せ連結処理に関しては、後に例を用いて詳述する。

【 0 0 2 9 】

問合せ連結を行うか否かの判定後、問合せ分配を行うか否かを判定する（ステップ604，605）。問合せ分配とは、一つの問合せを分解して、複数の協調するデータ中継機構で実行する方法で、上記処理によって問合せを発行したユーザと問合せの関係をサーバ計算機側のデータ提供システムから隠蔽することができる。問合せ分配に関しても、後に例を用いて詳述する。

## 【 0 0 3 0 】

問合せ連結を行い（ステップ 6 0 3 で Y e s が選択された場合）、かつ問合せ分配を行う場合（ステップ 6 0 4 で Y e s が選択された場合）には（b）連結－分配問合せを生成して（ステップ 6 0 7）問合せ変換ステップを終了する（ステップ 6 1 0）。問合せ連結を行い、問合せ分配を行わない場合（ステップ 6 0 4 で N o が選択された場合）には、（a）連結問合せを生成して（ステップ 6 0 6）問合せ変換ステップを終了する。問合せ連結を行わず（ステップ 6 0 3 で N o が選択された場合）、問合せ分配を行う場合（ステップ 6 0 5 で Y e s が選択された場合）には（c）分配問合せを生成して（ステップ 6 0 8）問合せ変換ステップを終了する。最後に、問合せ連結を行わず、問合せ分配も行わない場合（ステップ 6 0 5 で N o が選択された場合）には問合せを変換せずに問合せ変換ステップを終了する。

## 【 0 0 3 1 】

問合せ連結および問合せ分配処理について図 1 および図 8 を用いて説明する。先に説明したように、本実施例ではデータ中継機構に 2 つのクライアント計算機が接続されている。また、サーバ計算機上の情報提供システムの提供するデータは顧客の貯蓄額であるとする。

## 【 0 0 3 2 】

今、クライアント計算機 1（1 0 1）から問合せ Q 1（8 0 5）が、そしてクライアント計算機 2（1 0 2）から問合せ Q 2（8 0 6）が発行されたとする。この時、Q 1 と Q 2 の連結問合せは 8 0 7 に示すように、選択の対象は Q 1 の選択の対象である {顧客 I D, 支店, 貯蓄額} と、Q 2 の選択の対象である {顧客 I D, 貯蓄額} の和集合である {顧客 I D, 支店, 貯蓄額} となり、データベースに適用される条件（以下、問合せ条件と呼ぶ）は、Q 1 の問合せ条件 {貯蓄額  $\geq$  1, 0 0 0, 0 0 0} と Q 2 の問合せ条件 {貯蓄額  $\leq$  1 0, 0 0 0} を O R で連結した問合せとすればよい。

## 【 0 0 3 3 】

次に問合せ分配の方法を説明する。本実施例では、分配対象の問合せは連結問合せ 8 0 7 であるとしているが、分配の対象は連結前の問合せでも差し支えない

。本実施例では協調するデータ中継機構はデータ中継機構 1 0 5 および 1 1 4 の 2 つであるので、問合せ 8 0 7 を上記 2 つのデータ中継機構に分配する。2 つの分配問合せは、例えば分配問合せ D Q 1 ( 8 0 8 ) と、分配問合せ D Q 2 ( 8 0 9 ) のように構成でき、分配問合せ D Q 1 をデータ中継機構 1 0 5 で、そして分配問合せ D Q 2 をデータ中継機構 1 1 4 で実行させる。

## 【 0 0 3 4 】

上記分配の意味および目的は、問合せ 8 0 7 のうちの支店が新宿のレコードのみを D Q 1 としてデータ中継機構 1 0 5 で、それ以外を D Q 2 としてデータ中継機構 1 1 4 で実行させることにより、問合せ 8 0 7 の条件と発行元をサーバ計算機上で稼動する情報提供システムから隠蔽することである。

## 【 0 0 3 5 】

図 1 に戻って、問合せ変換部 1 0 7 で処理された問合せは暗号化問合せ生成部 1 0 8 に転送される。暗号化問合せ生成部では、入力された問合せに対する暗号化問合せを生成する。また暗号化プログラム生成部 1 0 9 では、前記暗号化問合せ生成部での暗号化方法に対応する暗号化プログラムを生成し、問合せおよび暗号化プログラム発行部 1 1 0 がネットワークインタフェース部 1 1 2 を介して、上記暗号化問合せ、および上記暗号化プログラムをサーバ計算機 1 1 9 に対して発行する。

## 【 0 0 3 6 】

暗号化問合せ生成部および暗号化プログラム生成部での処理を、図 1、図 4、図 9 および図 1 0 を用いて説明する。サーバ計算機 1 1 9 が提供する情報提供システムは遺伝子配列表 9 0 1 をデータベース 1 2 6 に保持しているとする。暗号化問合せ生成部 1 0 8 では、問合せ変換部 1 0 7 から転送された問合せを受け付け (ステップ 4 0 2)、隠蔽対象項目が存在するか否かを判定する (ステップ 4 0 3)。隠蔽対象項目が存在しない場合 (ステップ 4 0 3 で N o が選択された場合) には、暗号化問合せおよび暗号化プログラムを生成せずに暗号化問合せおよび暗号化プログラム生成処理を終了する (ステップ 4 0 7)。隠蔽対象項目が存在する場合 (ステップ 4 0 3 で Y e s が選択された場合) には、暗号化問合せを生成する (ステップ 4 0 4)。



## 【0037】

暗号化問合せとは、与えられた問合せのうち、隠蔽対象項目に指定された項目の値を暗号化した問合せである。例えば、暗号化問合せ生成部に転送された問合せがQ3（905）であり、前記遺伝子配列表の項目のうち、配列構造（904）が隠蔽対象項目として指定されているとする。この場合、上記問合せQ3で隠蔽対象項目である配列構造に対して指定されている値' a t c g ' を暗号化し、さらにデータの取得対象として配列構造を追加した暗号化問合せQ4（906）を生成する。ただし、暗号化問合せQ4（906）における、配列構造の値' @ 2 a S z E ' は' a t c g ' に暗号化を施した結果である。

## 【0038】

暗号化問合せでは、取得対象となるデータに、配列構造を追加している。これは、前記暗号化によって、暗号化前の値' a t c g ' と暗号化後の値' @ 2 a S z E ' が1対1の関係であることが保証されない場合に、取得した結果に対して、データ中継機構側で条件の再評価を行う必要があるためである。

## 【0039】

隠蔽対象項目に関する条件が「=」（等号条件）、もしくは「≠」（非等号）の場合には、値の暗号化方式として任意の暗号化を用いて差し支えない。ただし、隠蔽対象項目に関する条件が「<」、「≤」、「>」、もしくは「≥」（不等号）の場合に問合せ暗号化を用いる場合には、上記暗号化方式は大小関係を保持する暗号化方式を用いる。

## 【0040】

暗号化問合せを生成した場合には、暗号化プログラム生成の必要があるか否かを判定する（ステップ405）。暗号化プログラム生成の必要がない場合（ステップ405でN o が選択された場合）とは、暗号化プログラムとしてサーバ側に予め準備されたプログラム、もしくは暗号化プログラムサーバ129上の既存の暗号化プログラムを用いる場合であり、この場合には暗号化プログラムを生成せずに暗号化問合せおよび暗号化プログラム生成処理を終了する。暗号化プログラムを生成する必要がある場合（ステップ405でY e s が選択された場合）には、前記暗号化問合せに対応する暗号化プログラムを生成し（ステップ406）、

暗号化問合せおよび暗号化プログラム生成処理を終了する。

【0041】

図10を用いて暗号化プログラムについて説明する。隠蔽対象項目をTc(1001)、暗号化に利用する関数をfe()(1002)、暗号化前の値をvb(1003)、そして暗号化後の値をva(1004)と表すと、暗号化による問合せ条件の変換ステップは模式的に図10のようになる。この時、暗号化プログラム生成部109によって生成される暗号化プログラムは、データの検索対象となるサーバ計算機119のDBMS124内のデータアクセス部125で、暗号化関数fe()と同一の変換を行うプログラムである。

【0042】

上記プログラムは、前記DBMSが例えば(株)日立製作所のHiRDBのように、プラグインインタフェースを持っている場合には、上記インタフェース仕様を満足するプログラムでよい。また、前記DBMSがその内部にあるプログラミング言語の実行エンジンを搭載している場合には、上記プログラミング言語で記述したプログラムでも差し支えない。

【0043】

再び図1に戻って、暗号化問合せ生成部108および暗号化プログラム生成部109で生成された前記暗号化問合せおよび暗号化プログラムは、ネットワークインタフェース部112を介してサーバ計算機119に転送される。

【0044】

サーバ計算機119での問合せ処理を図1および図5を用いて説明する。サーバ計算機119のネットワークインタフェース部120では、暗号化問合せ115を受け付け(ステップ502)、上記暗号化問合せに対応する暗号化プログラムをサーバ計算機119が既に保持しているか否かをチェックする(ステップ503)。サーバ計算機119側で必要な暗号化プログラムを保持していない場合(ステップ503でNoが選択された場合)には、暗号化プログラム116を受信する(ステップ504)。上記暗号化プログラムを既に保持している場合には暗号化プログラム116の受信処理は必要ない。

【0045】

次に、前記暗号化プログラム116による暗号化済みデータがサーバ計算機119上に存在するか否かをチェックする（ステップ505）。上記データが存在する場合（ステップ505でYesが選択された場合）には、上記暗号化済みデータに対して検索処理を実行する（ステップ506）。暗号化済みデータが存在しない場合（ステップ505でNoが選択された場合）には、上記暗号化プログラム116をDBMS124内のデータアクセス部125に転送し、前記暗号化プログラム116を用いてサーバ側のデータを暗号化しながら検索処理を実行する（ステップ507）。

#### 【0046】

上記DBMSでは、受け取った暗号化問合せの隠蔽対象項目に対する値の復号を行わず、前記データアクセス部でデータベース126のデータを読み出す際に、前記暗号化プログラム116を用いて、上記データを暗号化しながら問合せと比較し、条件に適合するデータを検索結果122として抽出する（ステップ508）。

#### 【0047】

抽出した結果122の暗号化が施されていない項目に関して、その暗号化を行う場合（ステップ511でYesが選択された場合）には、前記暗号化プログラム116を用いて結果の暗号化を行い、データ中継機構105に上記結果を転送して（ステップ509）、サーバ計算機での問合せ処理を終了する（ステップ510）。結果の暗号化が不要な場合（ステップ511でNoが選択された場合）には、抽出結果を加工せずにデータ中継機構105に転送し（ステップ509）、問合せ処理を終了する。

#### 【0048】

検索結果122は、前記ネットワークインタフェース120を介してデータ中継機構105に転送される。例えば図9の暗号化問合せQ4がサーバ計算機に転送された場合を想定し、同時に転送された暗号化プログラムがf e l ( ) であったとする。この場合、前記DBMSではQ4を復号せずに実行し、前記データアクセス部が遺伝子配列表901のデータにアクセスする際に、配列構造のデータにf e l ( ) を作用させながら、Q4の配列構造= ' @ 2 a S z E ' に合致する

レコードを選択し、検索結果122としてネットワークインタフェース120、ネットワーク117経由で、データ中継機構105に転送する。

【0049】

データ中継機構105では、ネットワークインタフェース112を介して受け取った検索結果を結果統合部111で収集し、上記結果統合部111において結果統合処理を行う。

【0050】

図7を用いて結果統合処理について説明する。最初に結果に暗号化が行われた項目が含まれているか否かをチェックする（ステップ702）。暗号化された項目が存在する場合（ステップ702でYesが選択された場合）には、暗号化項目の復号化処理を行う（ステップ703）。次に問合せの暗号化処理が1:1変換であったか否かをチェックする（ステップ704）。暗号化処理が1:1変換でなかった場合（ステップ704でNoが選択された場合）とは、隠蔽対象項目の値を暗号化する際に、暗号化前の2つ以上の異なる値が、暗号化後には同一の値となる場合である。このような場合には、前記暗号化処理により、クライアント計算機から発行された問合せの条件を含むより大きな解の集合が結果として返されるため、サーバ計算機から取得したデータに対して、再度問合せ条件を適用し（ステップ705）、クライアント計算機から発行された問合せに対する正しい結果を生成する。

【0051】

暗号化処理が1:1変換であった場合（ステップ704でYesが選択された場合）には、問合せ変換部107で図6を用いて説明した問合せ変換処理が行われたか否かをチェックする（ステップ706）。問合せ変換が行われた場合（ステップ706でYesが選択された場合）には、クライアント計算機毎の正しい結果を生成する必要があるため、暗号化処理が1:1変換でなかった場合と同様に、サーバ計算機から取得したデータに対して、再度問合せ条件を適用する。問合せ変換が行われていなかった場合（ステップ706でNoが選択された場合）には、問合せ条件の再適用の必要はない。正しい結果を生成した後、生成した結果を問合せに対する解としてクライアント計算機に転送し（ステップ707）、

結果統合処理を終了する（ステップ708）。

【0052】

以上に例示した本発明の情報提供サービスによれば、ユーザからの問合せを受け付け、上記問合せに対するデータの検索結果を返す情報提供サービス方法において、ユーザの問合せに含まれる機密条件を解読しないことを高度に保証する情報提供サービス方法を提供することができる。

【0053】

また、本発明の応用によって、クライアント計算機システムからの問合せを受け付け、適切な情報提供サービスが稼動するサーバ計算機システムに問合せを転送する問合せ仲介サービス方法において、ユーザの問合せに含まれる機密条件を解読しないことを保証する情報提供サービスが稼動する前記サーバにのみ問合せを転送する情報検索での問合せ仲介サービス方法を提供することができる。

【0054】

また、上記本発明の実施による、クライアント計算機システムからの問合せを受け付け、適切な情報提供サービスが稼動するサーバ計算機システムに問合せを転送する、問合せ仲介サービスにおいて、複数の前記情報提供サービスの課金情報を収集して対価をまとめて支払い、その後前記クライアントの前記問合せ毎の課金情報を生成して、各クライアントに課金する情報サービス方法を提供することができる。

【0055】

【発明の効果】

本発明を用いることにより、情報提供サービスの利用者は自らが保護したい条件を隠蔽したままサービスを受けることができる。これにより、悪意のあるサーバ計算機の管理者に対して利用者の機密を保護することができる。

【図面の簡単な説明】

【図1】

本発明の一実施例におけるデータベースアクセスシステムを示すブロック図。

【図2】

従来例のネットワーク経由の暗号化問合せシステムのブロック図。

【図 3】

ネットワーク経由の問合せ処理方式の分類を示す説明図。

【図 4】

本発明の一実施例における問合せおよび暗号化プログラム生成の処理フロー図。

【図 5】

本発明の一実施例におけるサーバ計算機での問合せ処理を示すフロー図。

【図 6】

本発明の一実施例における問合せ変換処理のフロー図。

【図 7】

本発明の一実施例における結果統合処理ステップを示すフロー図。

【図 8】

本発明の一実施例における問合せ変換処理ステップの一例を示す説明図。

【図 9】

本発明の一実施例における問合せ暗号化処理の一例を示す説明図。

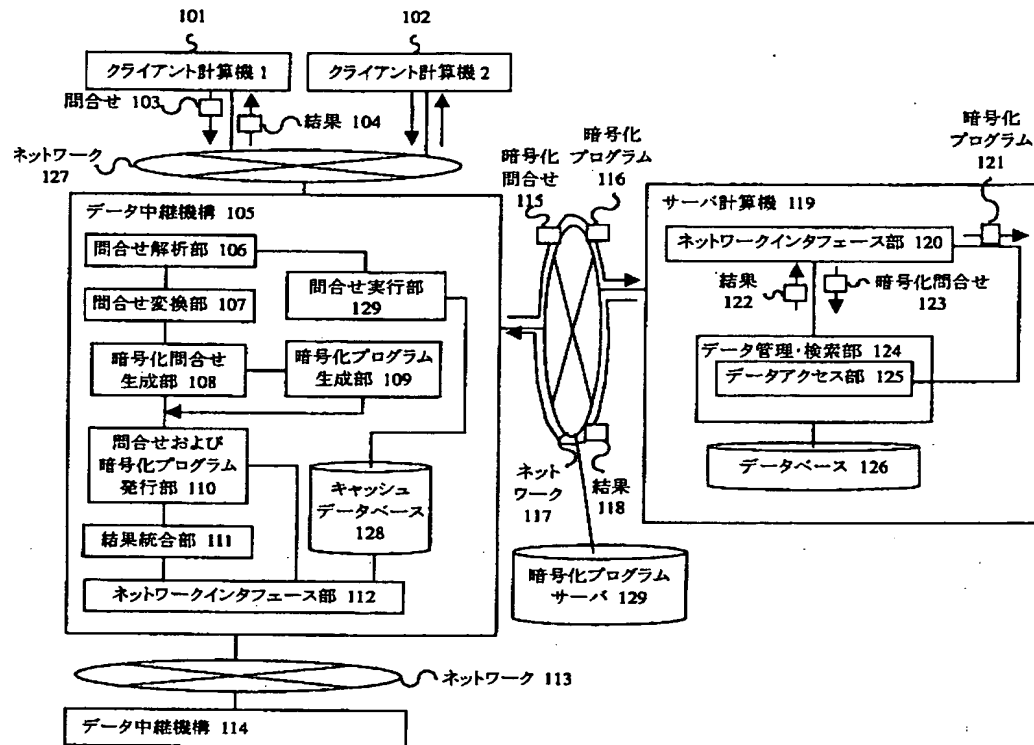
【図 1 0】

本発明の一実施例における暗号化処理の説明図。

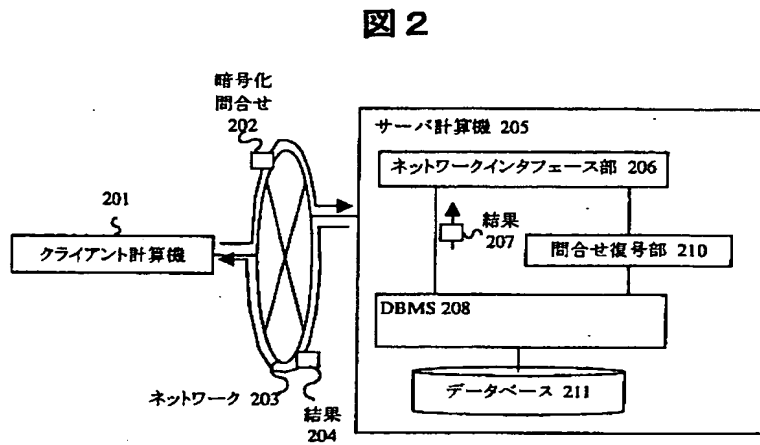
【書類名】 図面

【図 1】

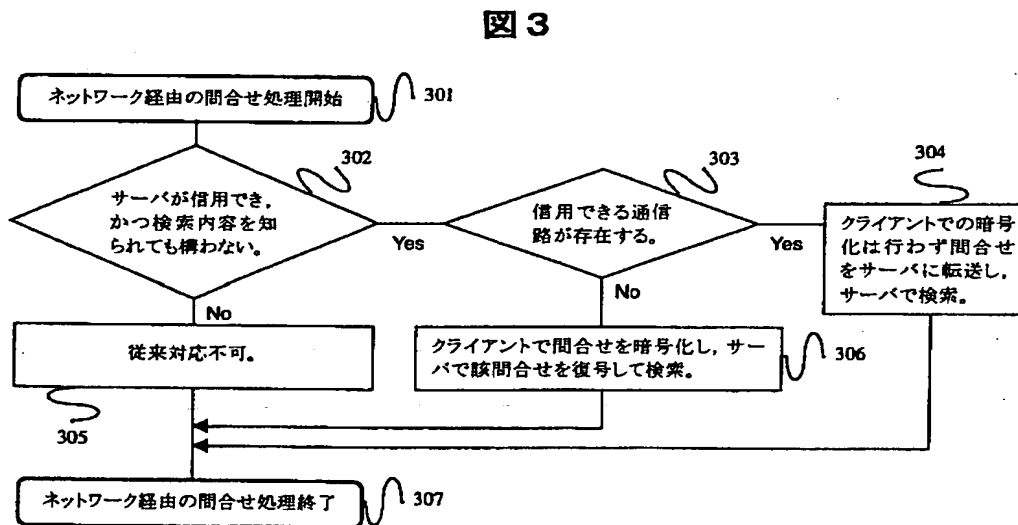
図 1



【図 2】



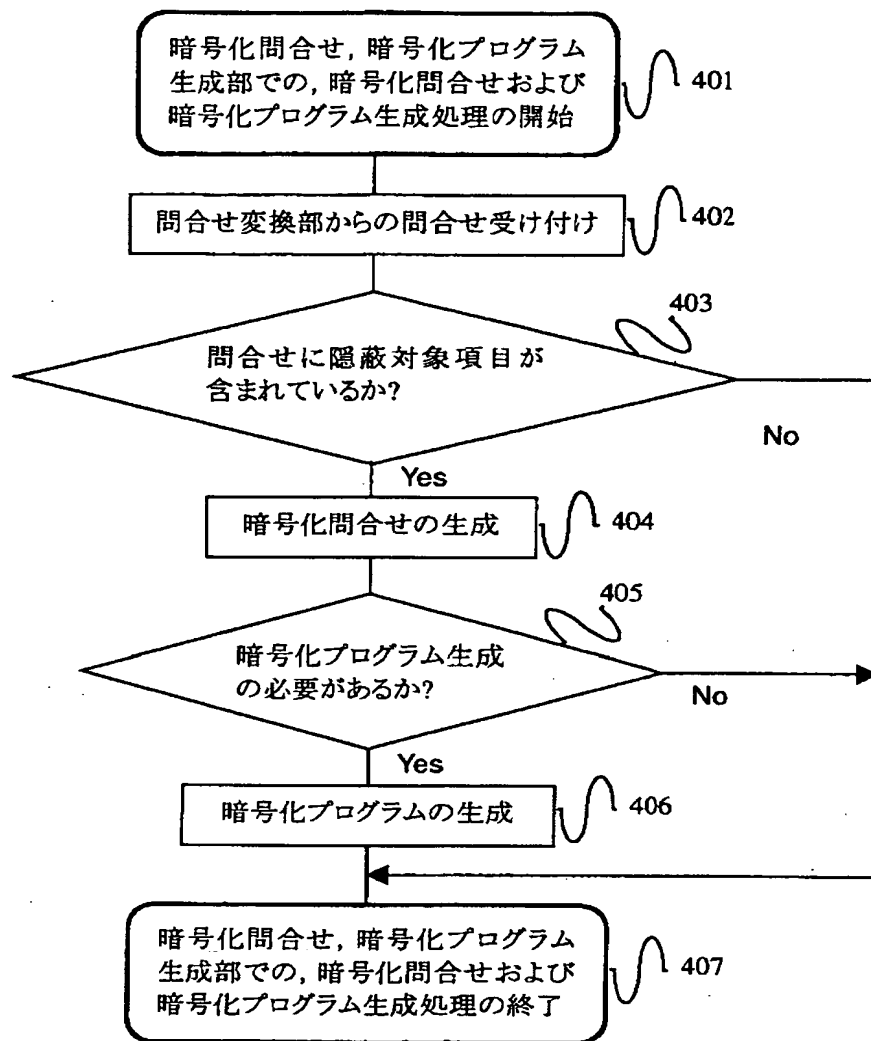
【図 3】





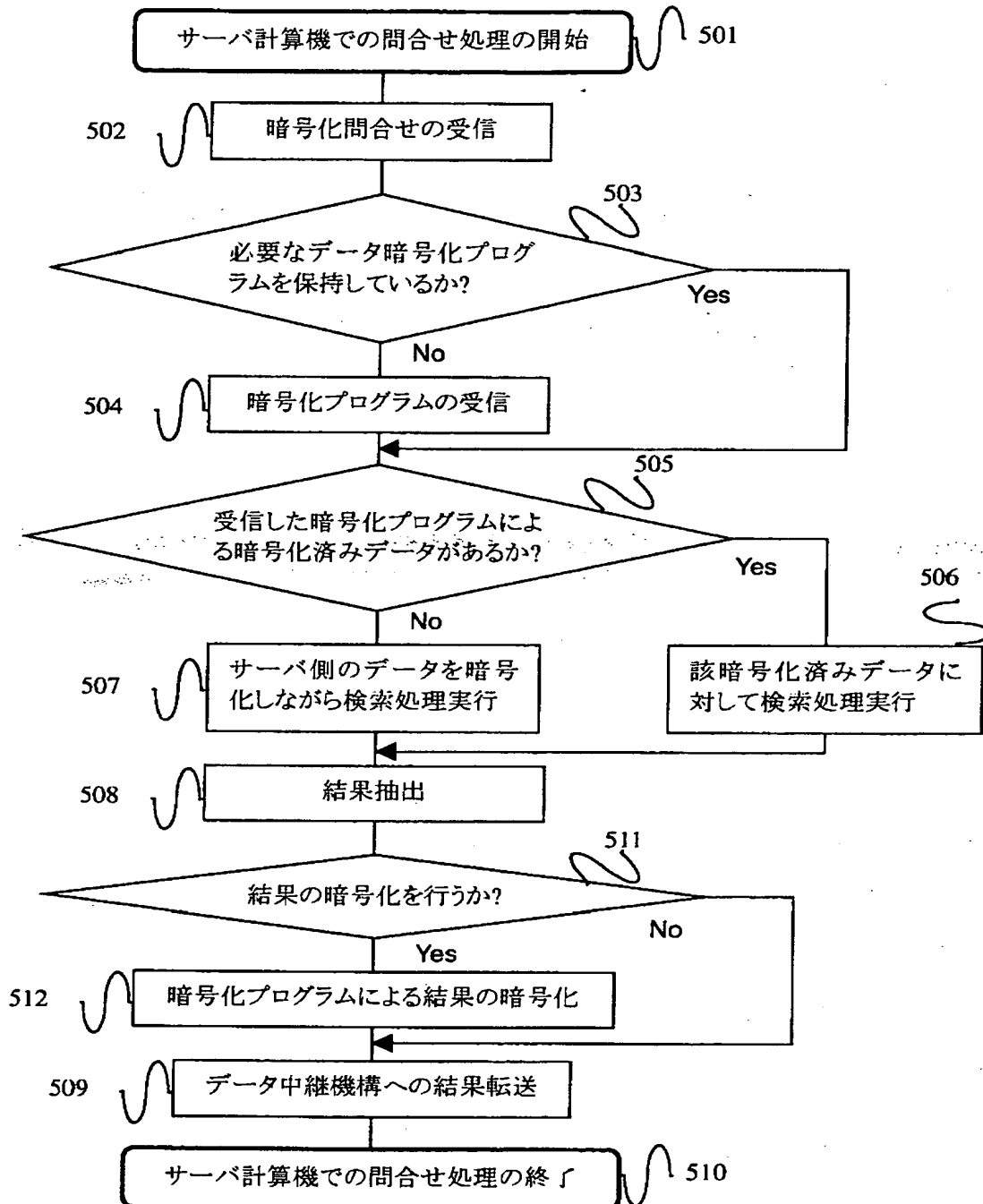
【図 4】

図 4



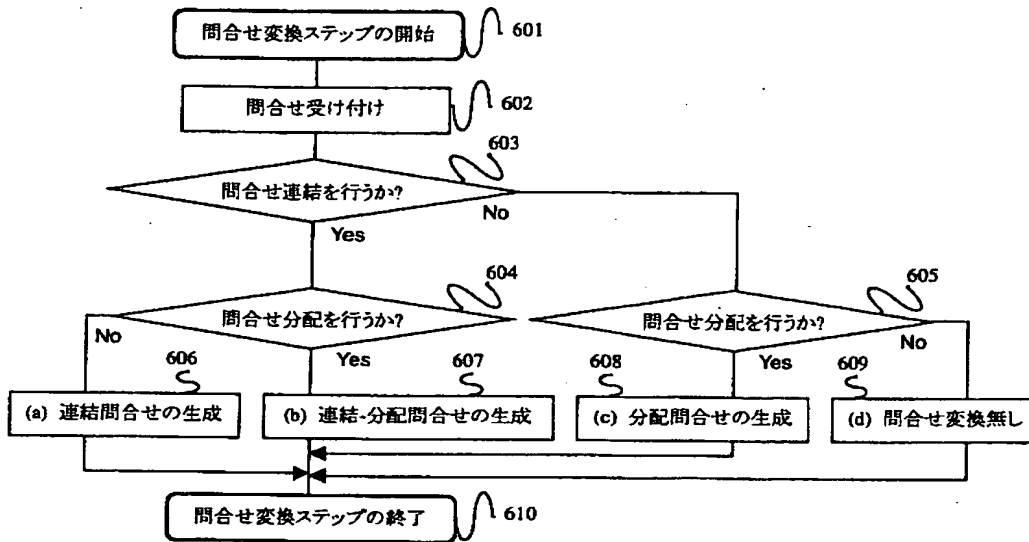
【図 5】

図 5



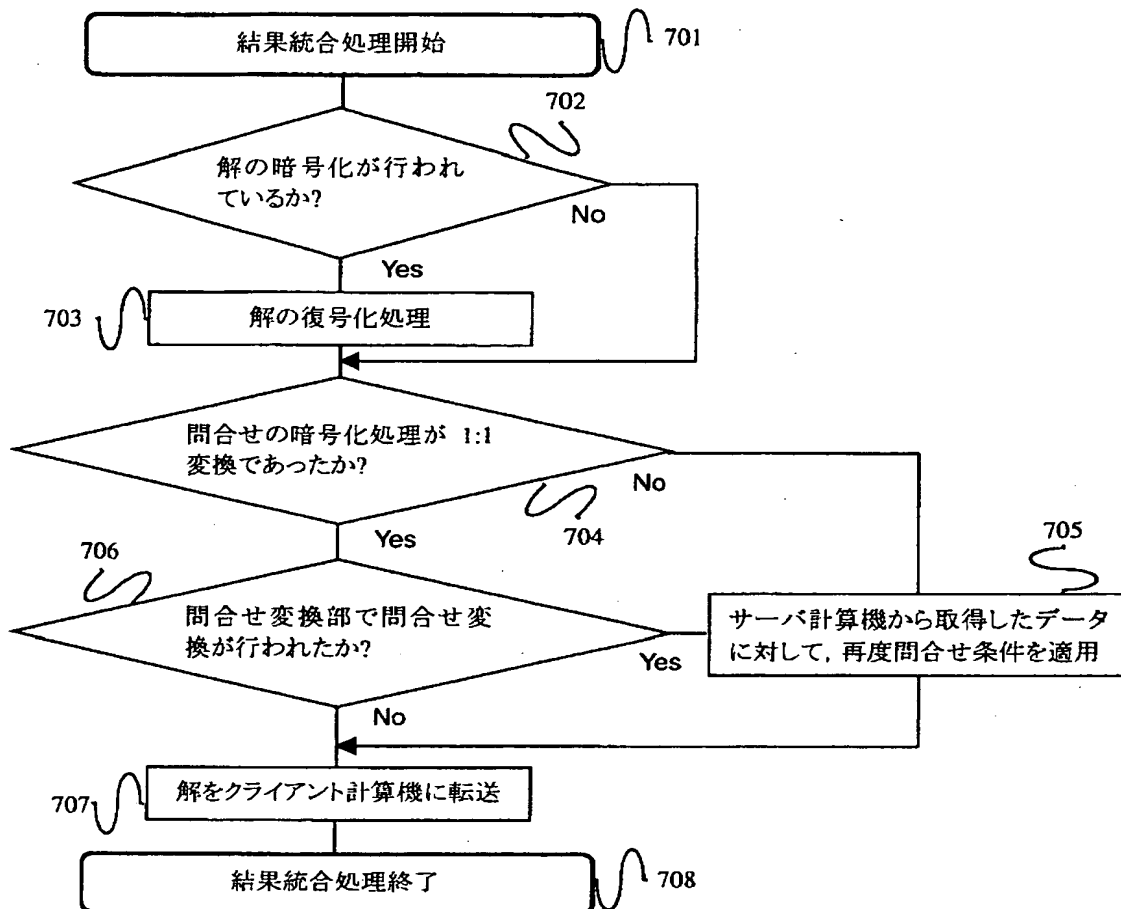
【図 6】

図 6



【図 7】

図 7



【図 8】

図 8

顧客 ID	支店	貯蓄額 (円)
060001895	新宿	1,050,000
061089288	池袋	125,000
060102952	新宿	120,000
...	...	...

貯蓄残高表 801

問合せ Q1:

```
SELECT 顧客 ID, 支店, 貯蓄額
FROM 貯蓄残高表
WHERE 貯蓄額 >= 1,000,000;
```

805

問合せ Q2:

```
SELECT 顧客 ID, 貯蓄額
FROM 貯蓄残高表
WHERE 貯蓄額 <= 10,000;
```

806

連結問合せ:

```
SELECT 顧客 ID, 支店, 貯蓄額
FROM 貯蓄残高表
WHERE 貯蓄額 >= 1,000,000 OR 貯蓄額 <= 10,000;
```

807

分配問合せ DQ1:

```
SELECT 顧客 ID, 支店, 貯蓄額
FROM 貯蓄残高表
WHERE (貯蓄額 >= 1,000,000 OR 貯蓄額 <= 10,000)
AND 支店 = '新宿';
```

808

分配問合せ DQ2:

```
SELECT 顧客 ID, 支店, 貯蓄額
FROM 貯蓄残高表
WHERE (貯蓄額 >= 1,000,000 OR 貯蓄額 <= 10,000)
AND 支店 <> '新宿';
```

809

【図 9】

図 9

名前	関連リンク	配列構造
abcd	site A	atcg
efgh	site B	tggtg
ijkl	site C	ccttt
...	...	...

遺伝子配列表 901

問合せ Q3:

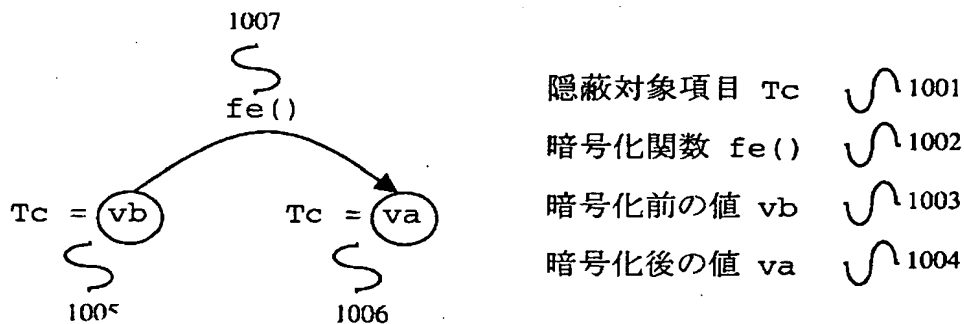
```
SELECT 名前, 関連リンク
FROM 遺伝子配列表
WHERE 配列構造='atcg';
```

問合せ Q4:

```
SELECT 名前, 関連リンク, 配列構造
FROM 遺伝子配列表
WHERE 配列構造='@2aSzE';
```

【図 10】

図 10



【書類名】 要約書

【要約】

【課題】 ユーザが保護したい条件を隠蔽したまま情報提供サービスを利用する方法およびシステム、さらに前記システムの性能を向上する機構を提供する。

【解決手段】 クライアント計算機に投入した問合せを変換し、上記問合せとサーバ計算機で実行される問合せの対応関係を変化させることで問合せ内容および問合せ発行位置を隠蔽し、問合せの暗号化対象項目を暗号化した暗号化問合せを作成し、サーバ計算機では上記暗号化問合せを復号せず、検索対象のデータを問合せと同様に暗号化しながら検索する。このとき、サーバ計算機に転送する暗号化プログラムを予め転送し、上記暗号化プログラム用の専用データを生成する、もしくはデータ中継機構内に問合せ結果をキャッシングする機構を準備し、問合せ処理で利用する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願2001-017827
受付番号	50100105773
書類名	特許願
担当官	第七担当上席 0096
作成日	平成13年 1月29日

<認定情報・付加情報>

【提出日】	平成13年 1月26日
-------	-------------



出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所